REMARKS

The Examiner rejects Claims 1, 3-4, 9, 11-12, 17, 19-20, and 25-27 under 35 U.S.C. 103(a) as being unpatentable under Warrender ("Detecting Intrusions Using System Calls: Alternate Data Models" IEEE Computer Society, Symposium on Security and Privacy, 1999, p. 133-145) in view of Cohen (U.S. Patent No. 5,481,650) and in view of Valente (U.S. Patent No. 6,779,120). Applicant respectfully disagrees with this rejection, especially in view of the amendments made hereinabove.

With respect to independent Claims 1, 9, and 17, applicant respectfully disagrees with the Examiner's contention that Valente teaches applicant's claimed "wherein selecting a rule for the valid behavior specification involves using an objective function that seeks to...minimize the number of possible system calls covered by the rule; wherein the objective function additionally seeks to minimize the number of privileged system calls covered by the rule" (see independent Claims, 1, 9 and 17). In rejecting applicant's claim language, the Examiner has relied, at least in part, on the following disclosure from Valente.

> "[D]eny access to all target principles via rules that identify initiators via the broadest possible credentials...then grant access to each target principle...to which access should be granted." (Col. 41 lines 50-54)

Applicant respectfully asserts that making a blanket rule, such as denying all access, and then making exception rules to the blanket rule, such as granting access to certain target principles, does not meet applicant's claimed rule involving an objective function that seeks to minimize the number of possible system calls covered by the rule and minimize the number of privileged system calls covered by the rule. Simply creating a blanket rule with exception rules would fail to give the same efficiency of applicant's claimed rule that meets the aforementioned specifically claimed multiple objectives.

Despite this clear distinction already present in the claims and in the spirit of expediting the prosecution of the present application, applicant now claims in each of the independent claims the subject matter of Claims 3, 11, and 19 below:

"wherein the objective function additionally seeks to minimize the number of privileged system calls covered by the rule and minimize a length of the rule" (emphasis added - see this or similar language in each of the independent claims).

The Examiner has rejected such subject matter of Claims 3, 11 and 19 under 35 U.S.C. 103(a), but has failed to cite any specific section of any reference under which applicant's claim language is rejected. Applicant respectfully asserts that neither Warrender, Cohen nor Valente teach selecting a rule with an objective function that, in part, seeks to minimize the length of the rule. Therefore, applicant requests an allowance or a specific prior art showing of such claim language.

In addition, the Examiner has rejected Claims 4, 12 and 20 under 35 U.S.C. 103(a), but again has failed to cite any specific section of any reference under which applicant's claim language is rejected. Again, applicant requests an allowance or a specific prior art showing of such claim language.

Regarding Claim 25, the Examiner has relied on the references cited with respect to Claim 1 to make a prior art showing of applicant's defined objective function. For the same reasons as argued in Claim 1 above, applicant respectfully asserts that Valente fails to even suggest an objective function that operates in the claimed manner. Further, the Examiner has stated that the equation presented in Claim 25 does not quantify any effectiveness of each individual parameter with respect to the explanation power and merely expresses that the objective function is characterized by three factors.

Applicant argues that incorporating the explanation power into the defined objective function allows the objective function to seek the highest possible explanation power while also seeking the lowest combination of generality, privilege and length of the clause. Therefore, the higher the value of the explanation power, the higher the value of the objective function and thus the more likely that a rule will be selected based on that objective function.

In addition, to define the objective function in order to further distinguish it over the prior art, applicant has added Claim 28 as described below which defines the explanation power.

With respect to Claim 26, the Examiner relies on the following excerpt in Cohen to make a prior art showing of applicant's claimed "wherein the values g_h and p_h are normalized to range from 1 to the total number of valid traces."

> "If positive examples remain, then the above process is repeated, as indicated by block 306, until the clauses in the hypothesis account for all the positive examples." (Col. 6 ,line 66-Col. 7, line 1)

Applicant respectfully asserts that Cohen's teaching of making sure that all positive examples are accounted for by the hypothesis clauses is not even a suggestion that the values of the generality and privilege of the clause range from 1 to the total number of valid traces. Applicant's claim language requires that both the generality and privilege of the clause include at least one trace that is explained by the rule up to the total number of valid traces, whereas the above excerpt from Cohen makes sure that all positive examples are accounted for.

With respect to Claim 27, the Examiner relies on the same rejection as that in Claim 25. Again, for the same reasons as argued in Claim 25, applicant asserts that nowhere in the prior art is there any suggestion of utilizing an objective function when selecting a rule, where a short, low-privileged and low-generality clause is favored while at the same time allowing the objective function to explain examples in many traces.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claim 28 below, which is presented for full consideration:

"wherein the explanation power is a number of valid traces that can be at least partially explained by the clause *h*" (see Claim 28).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P253/00.121.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100